iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61055

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Eclipse Preserving Differential Location Privacy Against Long-Term Observation Attacks

Sada Sai Kiran Reddy[1], Associate Prof. Dr. Ch. Srinivasulu[2]
Dept of CSE Institute of Aeronautical EngineeringHyderabad, India

Abstract: ***Mechanisms built around geo-in distinguish ability provide location privacy, allowing users to provide obfuscated locations for the Location-Based Service providers while still being able to use services appropriately. However, these systems are susceptible to inference attacks. An attacker, having prior knowledge of a user's disguised locations, can utilize long-term observation techniques to determine actual locations. Unfortunately, the question of how to guard against long-term surveillance assaults in differential location privacy is still unanswered. In this study, we first show the vulnerabilities as part of existing methods to long-term observation attacks. Given these vulnerabilities, we developed Eclipse, a unique technique that bridges the space between location protection and service usability. Specifically, we use geo-indistinguishability & k-anonymity to mask locations and hide them according to an anonymity set. As a result, our approach efficiently perturbs the spread of locations while suppressing leakage during long-term observation attacks. Furthermore, the collection of available outputs is used to minimize the influence on usability and accuracy. We officially define and rigorously establish the proposed mechanism's security via differential privacy. Furthermore, we develop the proposed approach and carry out several tests on real-life datasets to demonstrate its efficiency & efficacy.***

Keywords: Eclipse, Preserving, Differential Location Privacy, Long-Term Observation Attacks, Privacy Preservation, Location Privacy, Differential Privacy, Adversarial Attacks, Security, Anonymity

I. INTRODUCTION

Even though LBSs (Location-Based Services) provide significant convenience to users, they also raise serious privacy concerns because users' private locations [1] can easily be exposed [2] to the public [3],[4]. For example, a user must identify her exact address to find nearby pharmacies on Yelp. Multiple LPPMs (location privacy- preserving mechanisms) [5], [6], and [7] have been developed and proposed to protect users' location privacy. For example, geo-in distinct ability , which is generalized according to differential privacy [8], is capable of producing obfuscated locations around a radius to conceal a user's true position while still releasing approximated location information for preferred services. Existing geo- indistinguishable technologies[9] protect location privacy from attacks having no historical or prior information. However, recent research has demonstrated that, provided previous knowledge, an attacker can use inference attacks to reveal areas protected by these methods. For example, Yu et al. [10] explored privacy leaks using inference attacks, in which an attacker holds snapshots of an obfuscated location and previous information, also known as short-term observation assaults in this study. They show that leaks under short-term attacks are substantial and design an adaptive differential location privacy technique with personalized error boundaries called PIVE to reduce the leakage. Unfortunately, an attacker can circumvent our newly proposed defense by carrying out our recommended long-term observation attacks, Long-term observation assaults collect and preserve a user's behaviour over time, which can be used by adversaries to extract sensitive information through inference attacks. The behaviour in our attacks corresponds to the query requests delivered to the server, each of which comprises the user's obfuscated location as created by existent geo-in distinguish ability- based techniques. Once an attacker has a succession of disguised locations created by the same actual place (for example, home), he can use other prior information to determine the actual location. Millions of users follow the same daily habits (for example, at home, work, or school). Long-term observation attacks allow an attacker to easily uncover sensitive areas and infer users' interests and actions. It infringes on the confidentiality of millions of users and eventually undermines Internet freedom. The repercussions of these types of attacks are serious, and properly managing them is difficult. While randomly perturbing users' locations can easily prevent assaults, it hurts the usefulness and accuracy of location-based services. How can we close the privacy gap while also improving service usability? In this research, we suggest Eclipse, a novel location privacy- preserving technique, with an emphasis on overcoming such a challenge in Point of Interest (POI) search situations (e.g., Yelp & Foursquare). To address the issue, we combine geo- indistinguishability, k-anonymity, and predicted inferenceerrors.

©IJRASET: All Rights are Reserved

Specifically, our suggested approach uses geo- indistinguishability & k-anonymity to obscure the spread of locations while also promoting privacy against long-term surveillance threats. An obfuscated location hides in an anonymity set selected using k-anonymity. In addition, the collection of viable outputs is constructed by taking into account the Quality of Services (QOSS) restriction.As a result, Eclipse's disguised locations continue to provide approximated location details for desired services. In simple terms, our suggested technique protects privacy against long-term surveillance threats while having a low influence on theusefulness and veracity of LBSs.

II. EXISTING MODELS STUDY

Kido et al. [11] implemented a random walk model to generate dummy locations. The anonymity degree of this approach could beweaken if an adversary has prior information. To address this limitation, Niu et al. [12] proposed a new scheme to improve the generation of dummy locations. Liu et al. [13] selected dummy locations by evaluating the spatiotemporal correlation from three aspects, including time reachability, direction similarity and indegree/ out-degree. However, Zhang et al. [14] argued that a significant part of users may concern about their location privacy and therefore may not be interested in participating in an anonymity set. To solve this problem, they designed a set of auction-based mechanisms and proved that these mechanisms are truthful. In ongoing LBS questions, a few anonymity-based solutions have also been put forth. A privacy-preserving method against location injection attacks was suggested by Zhao et al [15]. Meanwhile, RobLoP, a robust privacy-preserving technique against location- dependent assaults, was presented by Jiang et al. [16]. Tang et al. [17] investigated the protection of long-term location privacy and put forth a series of innovative algorithms for generating dummy trajectories that take into account both long-term consistency and actual geographic data. A different technique was described by Beresford and Stajano
[18] to fend off long-term observation attacks, which involved regularly changing each user's pseudonym. However, if a user's preference data were kept on a server, an adversary could combine all the pseudonyms linked to requests for that user's data. Obfuscating the location data, maybe with noise or by reporting regions rather than points, is a crucial method for enhancing location privacy. As a result, we investigate long-term observational attacks against those processes that rely on geo-distinguishability. In order to provide differential privacy in a database that hasthe ability to do location pattern mining, Ho et al. [19] suggested a quadtree spatial decomposition. Differential privacy is not appropriate for applications where only one person is involved, even if it can be easily deployed in situations when the information of numerous users is aggregated.
In order to address this constraint, Dewri [20] put up a plan that blends k-anonymity with differential privacy. Additionally, it implied that there should be a similar likelihood of reporting the same obscured location from any of the k places. A paradigm-focused structure for indoor positioning that preserves privacy (P3-LOC) was also suggested by Zhao et al[21].

III. PROPOSED SYSTEM DESIGN AND DEVELOPMENT

A. Proposed System

The research introduces Eclipse, a novel technique aimedat preserving location privacy, particularly in Point of Interest (POI) search scenarios like Yelp and Foursquare. Eclipse combines geo-indistinguishability, k-anonymity, and predicted inference errors to address this challenge. It obscures location data while safeguarding against long-term surveillance threats. This is achieved by obfuscating locations within anonymity sets established through k- anonymity, while ensuring the Quality of Services (QOSS) requirements are met. Essentially, Eclipse protects privacy without significantly compromising the usefulness or accuracy of Location-Based Services (LBSs). The main contributions of this study are summarised as We create a long-term observation assault on existing techniques based on geo-in distinguishability. We identify the privacy drawbacks of various systems under long-term observation assaults. We developed a novel approach called Eclipse to improve privacy protection for a user's location. Eclipse incorporates k-anonymity, geo-indistinguishability, and predicted inference error, overcoming the limitations of previous investigations. It can successfully disrupt the propagation of disguised locations while having minimum impact on services. To the greatest extent of the knowledge we have, our approach is the first to protect against long-term surveillance assaults in the area of different location privacy. We formalize and rigorously establish Eclipse's security with divergent location privacy. To demonstrate the effectivenessand efficiency of our technique, we use Eclipse and run a series of tests on 2 real-world datasets (the Brightkite1 data set and the Gowalla2 data set) including several million location check-ins. Our findings imply that the suggested approach provides greater privacy than earlier options.

ADVANTAGES

In short, if the untrustworthy LBS provider has obfuscated locations, it can circumvent the confidentiality safeguards provided by location obfuscation methods and deduce a user's actual location using two forms of attacks:

Short-term Observation Attacks. In a short-term observation assault, the adversary can determine a user's true location with a snapshot of one disguised location plus additional prior knowledge. The preceding data regarding a specific user can be collected in a variety of ways, such using population density or the user's historical access information to a location-based service. Long-term Observation Attacks. Within a long-term observation assault, in addition to all the prior information discussed previously, an attacker can infer a user's actual position based on a succession of disguised user locations acquired by an adversary.

B. Employed an Algorithm An explanation of the suggestedprocedure

The actions required are

Step1: New user register by providing login informationStep2: Check user information on the server.
Step3: User authentication and validation.
Step4: People can sign in using their login credentials.Step5: Data sets are uploaded in Excel format.
Step6: Viewing the uploaded datasets is step six.
Step 7: Use the post type and hash code to identify location& attack type.
Step 8: Show the outcomes

C. Description About system modeling, design, anddevelopment

1) INPUT Design

Throughout the software development life cycle, input design is crucial and demands the utmost consideration fromdevelopers. The goal of the input design is to provide the application with accurate data. Thus, it is intended that inputs be efficiently designed to reduce errors that may arise during feeding. The input forms or screens are made to give users control over validation of the input limit, range, and other relevant validations, according to Software Engineering Concepts.

Input screens are present in nearly every module of this system. Error messages are designed to warn users of mistakes they make and point them in the correct direction to prevent the entry of erroneous data. Let's examine this in more detail under module design.

Putting user-created input into a computer-based format is called input design. Ensuring logical and error-free data entering is the aim of the input design. The input design controls the mistake in the input. The application has been designed with ease of use in mind. The way the forms are constructed, the cursor is automatically moved to the necessary entry location during processing. In some circumstances, the user is additionally given the choice to choose an appropriate input from a range of possibilities relating to the field.

Every piece of entered data must be validated. Once all of the entries on the current page have been made, the user can proceed to the next pages. An error notice is shown whenever a user submits incorrect data.

2) OUTPUT Design

The computer's output is needed mostly to establish an effective channel of communication within the organization, especially between the project manager and his team—that is, between the administrator and the clients. The system that the VPN produces enables the project manager to oversee his clients by adding new ones, assigning them new projects, keeping track of the projects' validity, and granting each client user-level access to folders based on the projects assigned to them.

The client may be given a new project to work on after one has been completed. Procedures for user authentication are upheld right from the start. The administrator alone is responsible for allocating projects and certifying new users. A user may register as a new user or the administrator may create one.

When an application is run for the first time, it launches. Internet Explorer is utilized as the browser after the server has been started. Since the project will be executed over a local area network, the other linked systems can function as clients and the server machine as the administrator. Even someone utilizing the system for the first time will find it to be very user-friendly and understandable.

3) MODULES

a) Administrator

In order to access this module, the service provider must enter a valid user name and password. Following a successful login, one can perform a number of tasks, including See Every User and Give Permission, See Every File Uploaded, See Every File UploadedBy Chain, See AllLong TermObservation Attackers, See All Attacker Outcomes, See All City Outcomes, See All Nation Outcomes.

b) View and Give Users Permission

The list of all registered users is viewable by the administrator in this module. This allows the admin to examine user information such name, email address, and address, and it also allows the admin to authorize people.

c) Final User

There are n numbers of users present in this module. Prior tobeginning any operations, the user must register. The user's information is saved in the database after they register. Upon successful registration, he must use his authorized user name and password to log in. The user will be able to perform many tasks after successfully logging in, including Register and Login, View Your Profile, Upload Datasets, View All Uploaded Datasets, Find Attacker Type, and Find Attacker Type By hash Code.

IV. DESIGN AND DESCRIPTION

Fig. 1 Depicts the architecture employed in this proposed work, including the admin, social server, end user, and database, as well as their respective features and roles. As shown in Fig. 2, a data flow diagram depicts how data will travel between the Social Server, System, and End User, as well as the relationships between them. Fig. 3 depicts a diagrammatic representation of actions conducted by the end user in the form of a flow chart, whereas Fig. 4 depicts steps performed by the social server.

1) Architecture

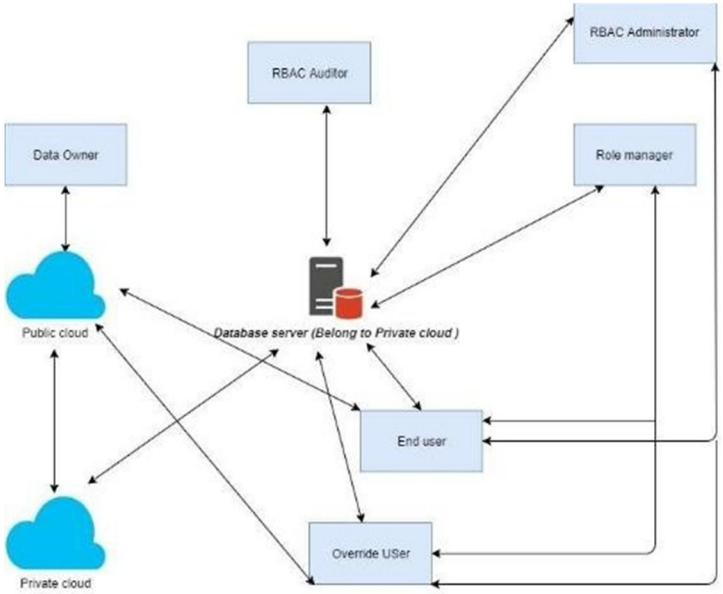


Fig. 1 Architecture

2) Data Flow

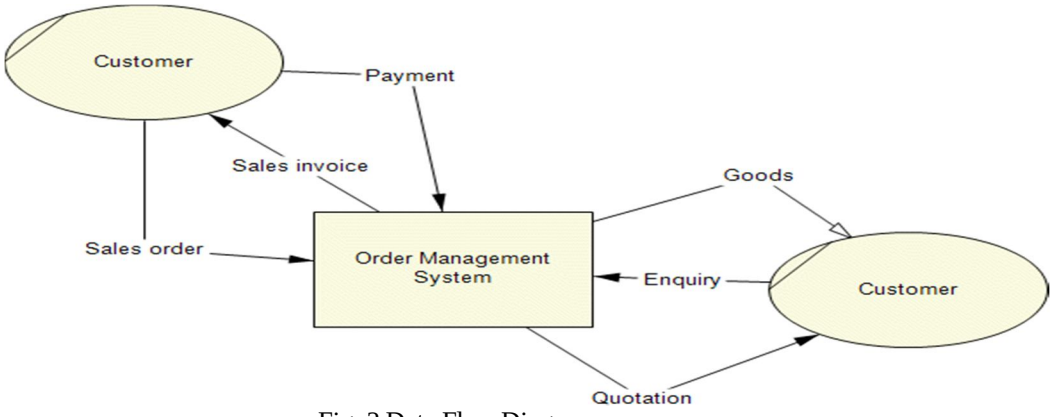


Fig. 2 Data Flow Diagram

3) Flow Chart

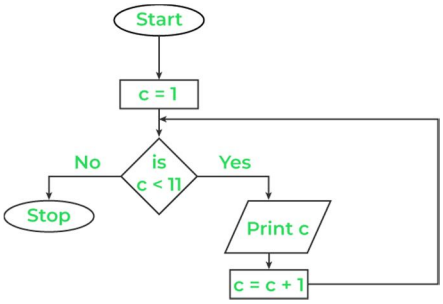


Fig. 3Flow Chart

4) Use Case

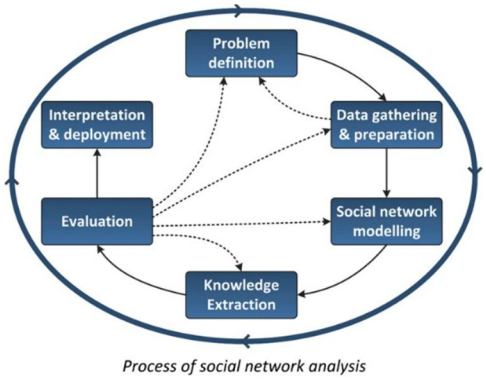
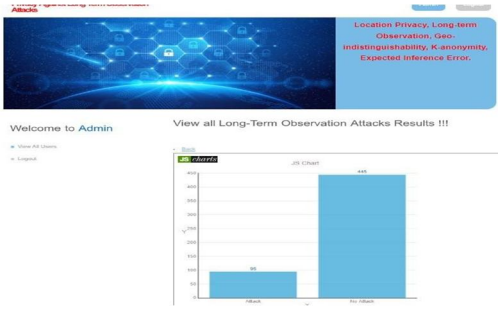


Fig. 4 Use Case

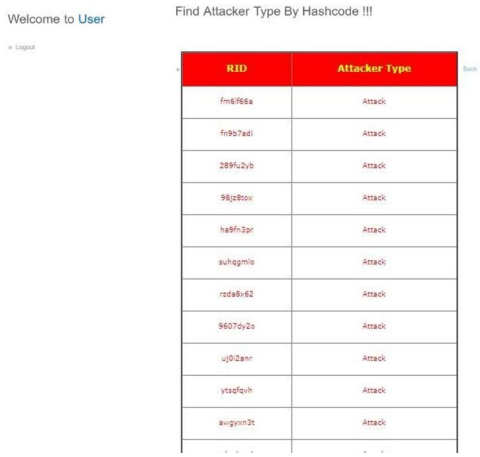
V. RESULTS AND DISCUSSION



©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |


Eclipse Preserving Differential Location Privacy Against Long Term Observation Attacks
Admin
Logout
Location Privacy, Long-term Observation, Geo-indistinguishability, K-anonymity, Expected Inference Error.
Welcome to Admin
View All Uploaded Datasets City Results !!!
View All Users
Logout
Back
JS charts
Location Privacy, Long-term Observation, Geo-indistinguishability, K-anonymity, Expected Inference Error.
Welcome to Admin
View All Uploaded Datasets Country Results !!!
View All Users
Logout
Back
JS charts
154
34


Eclipse Preserving Differential Location Privacy Against Long Term Observation Attacks
User
Logout
Location Privacy, Long-term Observation, Geo-indistinguishability, K-anonymity, Expected Inference Error.
Welcome to User
Find Attacker Details !!!
Logout
Enter RID
Enter Age
Enter Gender
Enter Latitude
Enter Longitude
Enter City
Enter Country
London
England
Find Attack


Welcome to User
Logout
Find Attacker Type By Hashcode !!!
Back
RID
Attacker Type
fm6lf66a
Attack
fn9b7adi
Attack
289fu2yb
Attack
98jz8tox
Attack
ha9fn3pr
Attack
auhqgmlo
Attack
rzda8x62
Attack
9607dy2o
Attack
uj0l2anr
Attack
ytqqfqvh
Attack
awgyxn3t
Attack


Eclipse Preserving Differential Location Privacy Against Long Term Observation Attacks
User
Logout
Location Privacy, Long-term Observation, Geo-indistinguishability, K-anonymity, Expected Inference Error.


Welcome to User
Logout
View Attack Found Status!!!
Long Term Observation Attacks Found Type
Attack
Back


Welcome to User
Logout
Find Attacker Type By Hashcode !!!
Back
RID
Attacker Type
pxymczn2
No Attack
a66sspp2
No Attack
9vnljm2r
No Attack
hnm54k4r
No Attack
7kzaglt2
No Attack
0d6o5w8z
No Attack
hiv576og
No Attack
k4l45ene
No Attack
10h2u1b1
No Attack
xckkdcl1
No Attack


Eclipse Preserving Differential Location Privacy Against Long Term Observation Attacks
User
Logout
Location Privacy, Long-term Observation, Geo-indistinguishability, K-anonymity, Expected Inference Error.
Welcome to User
Logout
Find Attacker Details !!!
Enter RID
fm9b7adi
Enter Age
39
Enter Gender
m
Enter Latitude
51.627072
Enter Longitude
-0.083648
Enter City
London
Enter Country
England
Find Attack

VI. CONCLUSION AND FUTURE SCOPE

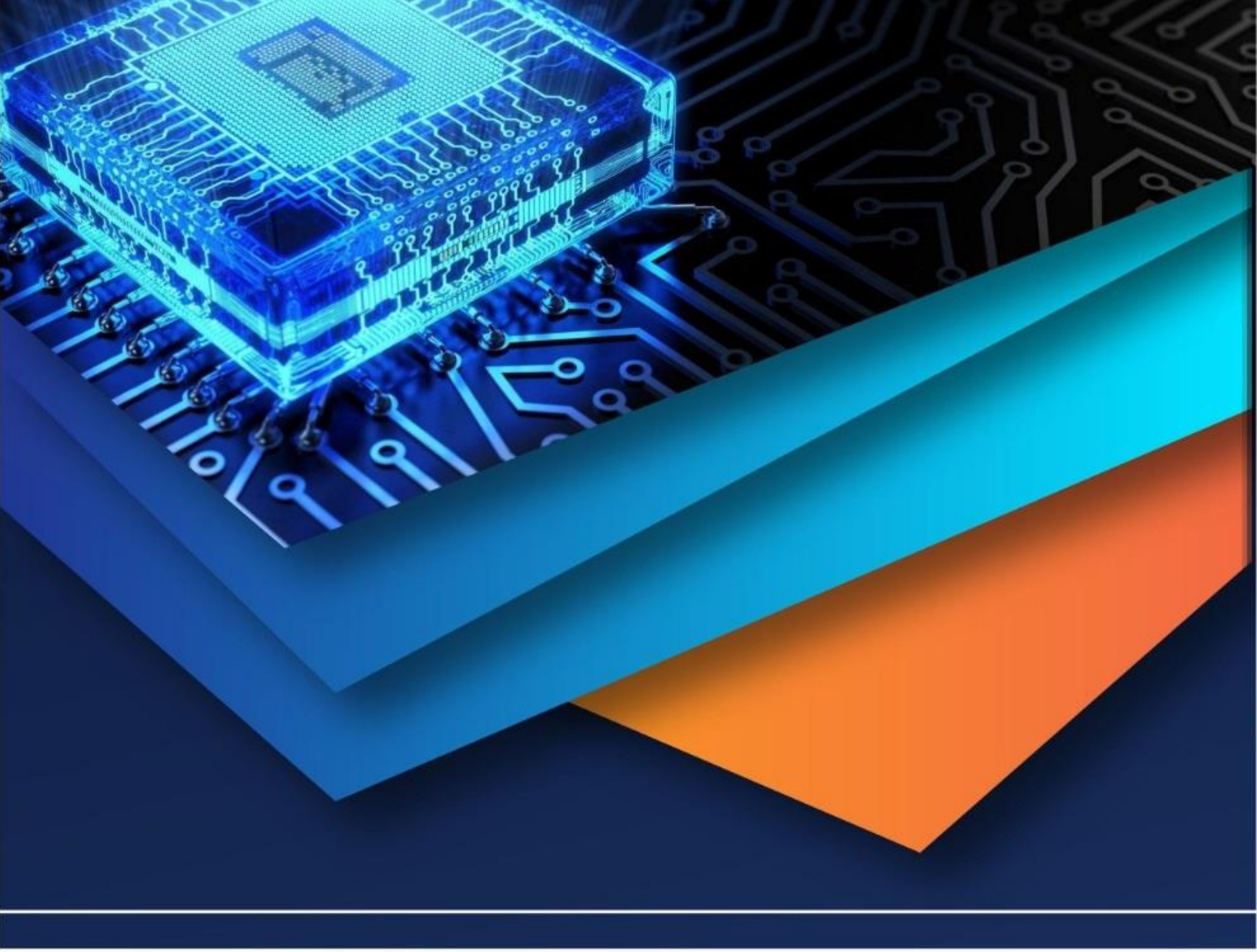
To successfully protect mobile users' location privacy from long-term observation threats, we introduced Eclipse, a three-phase differential location privacy-preserving method. Eclipse combines geo-distinguishability, k-anonymity, and anticipated inference error. Particularly, the set of possible outcomes determination phase begins by determining the user's QOS need. The anonymity set selecting step determines an anonymity group that ensures the desired inference error bound. At last, the combination of differential & anonymous location obfuscation process creates an obscured location that is both differential and anonymous. The evaluation results from two real-world datasets demonstrate our Eclipse's efficacy and efficiency.

VII. ACKNOWLEDGMENT

This Work has no Grants from Either private or public grants. There is no Conflict of interest between the authors. Authors Express thanks to All reviewers for their valuable remarks and suggestions.

REFERENCES

[1] H. Li, H. Zhu, S. Du, X. Liang, and X. S. Shen, “Privacy leakage of location sharing in mobile social networks: Attacks and defense,”IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4,pp. 646–660, 2018.
[2] Y. Zheng, L. Zhang, X. Xie, and W.-Y. Ma, “Mininginterestinglocations and travel sequences from gps trajectories,” in ACM WWW, 2009.
[3] H. Li, Q. Chen, H. Zhu, D. Ma, H. Wen, and X. S. Shen, “Privacy leakage via de-anonymization and aggregation in heterogeneous social networks,” IEEE Transactions on Dependable and Secure Computing,2017.
[4] L. Zhou, S. Du, H. Zhu, C. Chen, K. Ota, and M. Dong, “Location privacy in usage-based automotive insurance: Attacks and countermeasures,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 196–211, 2018.
[5] K. Fawaz, H. Feng, and K. G. Shin, “Anatomization and protection ofmobile apps location privacy threats,” in USENIX Security, 2015.
[6] K. Fawaz and K. G. Shin, “Location privacy protection for smartphone users,” in ACM CCS, 2014.
[7] Z. Montazeri, A. Houmansadr, and H. Pishro-Nik, “Achieving perfect location privacy in wireless devices using anonymization,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2683–2698, 2017.
[8] C. Dwork, “Differential privacy,” in Springer ICALP, 2006.
[9] M. E. Andr´es, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, “Geo-indistinguishability: Differential privacy for location-based systems,” in ACM CCS, 2013.
[10] L. Yu, L. Liu, and C. Pu, “Dynamic differential location privacy with personalized error bounds,” in ISOC NDSS, 2017.
[11] H. Kido, Y. Yanagisawa, and T. Satoh, “An anonymous communication technique using dummies for location-based services,” in IEEE ICPS, 2005.
[12] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, “Achieving k-anonymity in privacy-aware location-based services,” in IEEE INFOCOM,2014.
[13] H. Liu, X. Li, H. Li, J. Ma, and X. Ma, “Spatiotemporal correlationaware dummy-based privacy protection scheme for locationbased services,” in IEEE INFOCOM, 2017.
[14] Y. Zhang,W. Tong, and S. Zhong, “On designing satisfaction- ratioaware truthful incentive mechanisms for k-anonymity location privacy,” IEEE Transactions on Information Forensics and Security,vol. 11, no. 11, pp. 2528–2541,2016.
[15] P. Zhao, J. Li, F. Zeng, F. Xiao, C. Wang, and H. Jiang, “Illia: Enabling k-anonymity-based privacy preserving against location injection attacks in continuous lbs queries,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1033–1042, 2018.
[16] H. Jiang, P. Zhao, and C. Wang, “Roblop: Towards robust privacy preserving against location dependent attacks in continuous lbs queries,” IEEE/ACM Transactions on Networking, vol. 26, no. 2, pp. 1018–1032, 2018.
[17] F. Tang, J. Li, I. You, and M. Guo, “Long-term location privacy protection for location-based services in mobile cloud computing,” Soft Computing, vol. 20, no. 5, pp. 1735–1747, 2016.
[18] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” IEEE Pervasive computing, no. 1, pp. 46–55, 2003.
[19] S.-S. Ho and S. Ruan, “Differential privacy for location pattern mining,” in ACM SPRINGL, 2011.
[20] R. Dewri, “Local differential perturbations: Location privacy under approximate knowledge attackers,” IEEE Transactions on Mobile Computing, vol. 12, no. 12, pp. 2360–2372, 2013
[21] P. Zhao, H. Jiang, J. C. Lui, C.Wang, F. Zeng, F. Xiao, and Z. Li, “p3- loc: A privacy-preserving paradigm-driven framework for indoor localization,” IEEE/ACM Transactions on Networking, vol. 26, no. 6,pp. 2856–2869, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)